THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 18: Issue 16

Saturday 1 June 1996

Contents

Xerox machine caused nuclear power plant emergency halt

Magnus Ihse <d95-mih@nada.kth.se>
Thu, 30 May 1996 13:16:56 +0200 (MET DST)

One of the Swedish nuclear reactors, Ringhals 4, was automatically shut down during a routine safety check. The last part of the instructions fed into the computer was missing, and when the computer safety system noticed that the instructions were incomplete, it shut down the reactor.

So far so good, but why were the instructions incomplete? The Xerox machine used to copy the instruction sheet did not include the complete page, and no one (except the computer) ever noticed that the instructions were incorrect. (Source: TT)

The risk is obviously that no system is completely fool-proof. I doubt anyone ever thought about the correctness of the Xerox machines as part of the nuclear power plant safety system. No matter how detailed you planned the security system, there will always be some part that could fail. In this case, nothing serious happened because the computer detected the error. However, this -- or similar incidents -- could happen again, and next time maybe the error would not be detected.

Magnus Ihse, Computer Science student, Royal Institute of Technology, Sweden

---

✓ NY Air Route Traffic Control Center computer failure

Peter Ladkin <ladkin@TechFak.Uni-Bielefeld.DE>
Thu, 23 May 1996 21:28:10 +0200

The NY ARTCC computer (7 years old) lost significant service capability (`failed' said the NYT Service's Matthew Wald on 21 May 1996) twice on the evening of Monday 20 May; the first time for 23 minutes, and the second time for about an hour, one hour later. The NYTS reported (International Herald Tribune, Thurs 23 May 1996 p2) that it was `running normally' Tuesday as technicians tried to figure out the problem. The FAA is wondering about the new software installed four days earlier.

`The office, the New York Air Route Traffic Control Center, handles high-altitude and long-distance traffic over New York, Connecticut, New Jersey, Pennsylvania and part of the Atlantic Ocean.' (Wald, NYTS, 21 May 1996)

There followed the usual: a fail-safe return to older, more inefficient air traffic control procedures, leading to a lower traffic saturation limit and thus mean delays in departures of about an hour at major airports in the area; an increase in the work load of controllers; a deficit of safety-related information, including `automatic conflict alert'.

I note that a deficit of safety-related info does not necessarily lead to a reduction in safety: one increases safety margins and pays careful attention (which might even increase safety for the short periods involved). These older procedures worked tried and true for decades. Risks might increase were an ARTCC system to suffer a service reduction at a time at which there were more aircraft in the system than the saturation limit for the reduced level of service. Aircraft in the air already under control do not just go away, however one can delay entry into Center control by delaying aircraft ready for departure and diverting flying traffic due to enter Center control (but note the huge area NY ARTCC covers). I am

not aware that such a circumstance has ever occurred, but given the projected growth in commercial air traffic, it is something to worry about for the future.

Computers and ATC were discussed in RISKS-17.17 (James), 17.18 (Wolper), 17.21 (Burstein, Schultz), 17.24 (PGN), 17.25 (Runes, Karagianis, Ladkin, Pettit), 17.26 (PGN, Margolin, Zellweger), 17.27 (Gelato), 17.28 (PGN), 17.35 (Lucero), 17.36 (Tignanelli, 2 articles), 17.38 (Ladkin), 17.40 (PGN, Ladkin), 17.41 (Tignanelli, Emerson), 17.44 (Goldstein, see also Harding, Menon), 17.49 (PGN), 17.50 (PGN), 17.62 (Kabay), 17.70 (Wolper). It seems as if 1995 was a good vintage ... [Especially if you don't wine too much. PGN]

ATC Communications were discussed in 17.44 (Harding, Menon), 17.64 (Lucero), 17.65 (Ladkin).

Peter Ladkin

✍ US Charges Man Planned to Kill 4,000 Travelers (Reuter)

"Peter G. Neumann" <neumann@csl.sri.com>
Fri, 31 May 96 15:46:42 PDT

Reuter reported on 29 May 1996 that U.S. prosecutors accuse Islamic militant Ramzi Ahmed Yousef (a.k.a. Abdul-Basit Balochi) and two others of plotting to bomb 12 U.S. jet planes in two days during 1995. Some of the evidence is based on a file found in Yousef's laptop computer, stating that the purpose of the bombings was ``vengeance and retribution'' against the United States for its financial, political and military support of Israel. (Yousef will be tried later this year for masterminding the 1993 World Trade Center bombing that killed six and injured more than 1,000 people. He is also accused of placing a bomb on a Philippine Airlines flight from Manila to Tokyo on 11 Dec 1994, which killed one passenger and injured 10 others.)

✍

Ken Knowlton <KCKnowlton@aol.com>
Fri, 31 May 1996 12:00:000001 pm EDT

Responses to my 12 am/pm = noon/midnight? were mostly of these three forms:

1. 12 am is midnight, dummy; don't bother me with this.
2. Either can mean either; don't use these notations.
3. Tuesday goes from "12am Tues" to "midnight Tues" (and 12am = midnight)!

My conclusions:

1. Be careful in making assumptions about other people's assumptions.
2. I bet that somewhere in this world there's a routine that occasionally time-stamps with the ASCII string "... 12:00 am" and a backup, restore or merge routine that later misunderstands the date (misidentifying

the most recent version of a file, or whatever).

I think I can demonstrate how easy it is to make risky assumptions about other people's assumptions, particularly regarding the phenomenon "don't need this case -- it just couldn't get here." We all know what scalene and isosceles and equilateral triangles are, likewise we have crisp ideas about squares, rhombuses, rectangles, parallelograms and trapezoids, yes? I invite you to demonstrate to yourselves your knowledge of inclusion/intersection/exclusion relations among these objects by filling in each of the following blanks with a 'No' or 'Some' or 'All'. Use your own self-assured knowledge here -- don't use a dictionary or other authority. Please *don't* send me your answers unless you can fill in all the blanks exactly as you think every responsible geometrician would. Assume that all figures are planar and non-degenerate:

No/Some/All
____ equilateral triangles are isosceles triangles.
____ equilateral triangles are scalene triangles.
____ isosceles triangles are equilateral triangles.
____ isosceles triangles are scalene triangles.
____ scalene triangles are equilateral triangles.
____ scalene triangles are isosceles triangles.
____ squares are rhombuses.
____ squares are rectangles.
____ squares are parallelograms.
____ squares are trapezoids.
____ rhombuses are squares.
____ rhombuses are rectangles.
____ rhombuses are parallelograms.
____ rhombuses are trapezoids.
____ rectangles are squares.
____ rectangles are rhombuses.
____ rectangles are parallelograms.
____ rectangles are trapezoids.
____ parallelograms are squares.
____ parallelograms are rhombuses.
____ parallelograms are rectangles.
____ parallelograms are trapezoids.
____ trapezoids are squares.
____ trapezoids are rhombuses.
____ trapezoids are rectangles.
____ trapezoids are parallelograms.

Ken Knowlton

[... and Ken is NOT a square. While at Bell Labs in the 1960s, his programming language BEFLIX pioneered computerized animation; he also did L6, among other things. PGN]

↗ re: TILT! Counterfeit pachinko cards ... (Wayner, RISKS-18.15)

Chiaki Ishikawa <ishikawa@personal-media.co.jp>
Tue, 28 May 1996 22:09:28 +0900 (JST)

I would like to add some background as someone who has played in pachinko parlors in Japan. (The origin of the game of pachinko is rather vague. Some say it is based on the ball game popular after the WW-II in U.S.A.. Anyway, it is a gambling business.)

The card in question acts as a kind of debit card inside the pachinko parlors. It was introduced a few years ago by an former police official, with the expressed intention of keeping the money flow easy to track. (I would say it was a ruse to make a few companies where the ex-police officials can find jobs after retirement from the office. But I digress.)

The cards are sold to the pachinko parlors and the customers buy the cards from the parlors, and obtain steel balls to play the game by inserting the card into the slot next to the game machine.

Pachinko gambling works as follows. When you win the game, the number of steel balls in your possession increases and the customer can exchange the balls with gifts. (Therein lies a complication. Japanese law prohibits gambling, and so exchanging the steel balls with real money is illegal. *However*, first exchanging the balls with gifts, and then exchanging the gifts with money at a third party outlet [which is quite likely to be operated by the parlor owner] has been allowed by the police.) Speaking of loophole! Some people do bring back the gifts to homes: depending on the places, parlors carry game-boy cartridges, latest bestseller books, snack food such as cookies, instant noodles, umbrella, purse, movie video tape, music CD, to name a few as gifts. But if the customer wants to exchange his/her win indirectly to money at the outlet, then he/she has to ask for special gifts used essentially as money tokens by these establishments. These are often a tiny gold/silver foil embedded in thin plastic slab, etc.. Each parlor/outlet pair uses different stuff. In my hometown, a special brand of silk stocking was used as money token. This whole thing is a farce in view of the anti-gambling law in Japan.)

Back to the card: the cards in question are used by two leading card manufacturers. (There are another couple of late-entry companies whose cards are not known to be attacked yet.) The card is based on the design done by NTT Data. NTT is the Japanese equivalent of old Ma Bell in the USA. NTT Data is a company that specializes in computer software integration, communication and such. I believe it designs the telephone card (debit card used for pay-phone in Japan), too.

The pachinko card is the size of name card and plastic. The details are not published. To the best of my knowledge, I think there is a magnetic strip that contains the card ID information such as its serial number and the amount of debit money.

There were 10,000 yen, 5,000 yen, 3,000 yen, 2,000 yen, and 1,000 yen cards. (I said "were" because 10,000 yen and 5,000 yen cards are no longer available.)

Attack method:

>From what I saw and read, the first card verification mechanism used by the pachinko game machine was so primitive to defy rational explanation: each time the card was used, a tiny hole was punched to indicate the amount left in the card. As the customer uses the card, the position of the punched hole on card shifts toward the zero position. Once there is a hole on the zero position, the card is no longer usable.

The first simple attack as far as I can tell was to fill in the hole in the

card with tiny plastic (essentially the chaff produced when the hole is punched was used to fill in the hole). I am not sure if such simple attack was possible, but it seemed possible really at the beginning with crude modification of the magnetic data.

Then, of course, the magnetic information on the card was also modified in more sophisticated ways when the card was used.

However, the bad people also learned and somebody stole the reader mechanism and figure out the part of the magnetically-coded information: the result was that bad people could buy the pristine 10,000 yen card and then uses up to 2500 yen of the debit amount legally and then "re-fill" the card to 9500 yen worth, thus gaining 2000 yen for free again and again. (Until 3000 yen was used from the 10,000 yen card, the physical hole was not produced on the card, and only the magnetic information was changed. Hence the mere counterfeiting of the magnetic information was necessary to "revive" the card. No physical re-filling of the card was necessary. Physically re-filling the hole is easy to spot visually and was avoided by the bad guys.)

[I have to confess that the exact amount involved in the counterfeiting is a little uncertain. But the general idea still holds.]

Similar attack was possible with 5,000 yen card.

Presumably the gain by attacking 3,000 yen, 2,000 yen and 1,000 yen card was small compared with the risk, the bad guys didn't attack these cards until lately.

Now the situation is that of cats and mouse. New counterfeiting methods and counter-measures follow each other in rapid succession.

I believe that the cloning of the card was also done. But I don't know the details.

Now, the card companies and pachinko parlors stopped issuing 10,000 yen and 5,000 yen cards because the damage was so large.

Also, they have installed special readers to verify the validity of the card by incorporating more vigourous checking not available on the readers next to the game machine: it used to be that the cards sold could by used by any pachinko parlors in Japan. Now cards sold elsewhere have to be verified with this machine before used at a local game parlor. Cards sold at the local parlor can be used without such checking.

Already, there are reports of counterfeit-card usage:

- either the cards are so sophisticated that they can pass the enhanced reader.
- Or the bad guys buy the cards locally and then use some of the debit amount and then bring the cards to their factory to re-fill and re-use it at the local store again and again.

The card companies have installed countermeasures in selected stores to the cloning of the card by checking the serial number of the card and stopped the operation of the whole game machines in the store if a card with the serial number of the previously used (finished?) card is ever inserted into the game machine.

Another simple method of fooling the reader was also reported about a month

ago. Essentially, it cuts out a long strip of the 3,000 yen card (now the most expensive card after 10,000 yen and 5,000 yen card are gone) and rotates the strip to invert its direction and then reassembles the card again using cement or something. To my surprise, it was reported to be deemed valid by some readers (!?). Apparently some readers only check for the position of the hole on fixed position and fooled to believe the card is valid if the hole is not in the expected position, etc.. Once not so rigorous readers are distributed, it is very difficult to upgrade all of them in Japan, I guess.

The problem is complicated in that the counterfeiting only damages the card company. The parlors report the amount of debit money used in their shops and then compensated for the amount (less the small surcharge by the card company.) This means that every time the counterfeit card is used the card company alone loses money and the local parlor doesn't lose.

There have already been reports of the owners of the pachinko parlors involved in the usage of the counterfeit cards. These bad owners allowed the bad guys to use the counterfeit cards in their parlors and pass the used debit amount to the card company and getting compensated.

In these cases, the bad guys bring back the money (by simply exchanging the phony debit money into the steel balls, and then without playing (they can play if they wish), exchange the steel balls to the special gifts, and then exchange the gifts with money. [Usually, buying the steel balls and then exchanging them with gifts, and subsequently with money leaves you less money than you started with. The house always wins. In this case, the bad guys started out with counterfeit debit money and ends up with real money, so it is OK for the bad guys.] The parlor also gets the money for the used debit money. So they win, too. Only the card companies lose.

Counterfeiting probably has existed since the first money (or equivalent) was ever invented. But, it surprised me that NTT Data approached the whole scheme so naively, especially since there have been reports of telephone card counterfeiting in Japan before. Some of the counterfeiting methods reported seemed so simple, and I have a doubt whether NTT Data was serious enough to deter counterfeiting.

At least, I can safely say they have underestimated the ingenuity of the counterfeiters badly and didn't learn from the counterfeiting of telephone cards very well.

Ishikawa, Chiaki (family name, given name)
Personal Media Corp., Shinagawa, Tokyo, Japan 142 ishikawa@personal-media.co.jp

---

Timing out e-mail -- "kidsciencenet" spam

Laurence Brothers <quasar@bellcore.com>
Wed, 29 May 1996 11:18:38 -0400

I recently received the following (names deleted to protect the possibly innocent):

> Subject: kidsciencenet

> Hi, our names are XXXXX and XXXXX. We are in the 5th grade at the
> XXXXXXXXXXXXXXXXXXXXXXXXXXXXX, Massachusetts, USA. We are
> doing a science project on the Internet. We want to see how many
> responses we can get back in two weeks. (We are only sending out 2
> letters).
>
> Please respond and then send this letter to anyone you communicate
> with on the Internet. Respond to XXX@tiac.net.
>
> 1. Where do you live (state and country)?
> 2. From whom did you get this letter?
>
> Thank you,
> XXXXXXXXXXXXXXX

I did NOT delete any original mail headers; the only headers were those of some intermediate remailers who had forwarded only the contents of the "original" note.

God help the ISP for tiac.net if this thing spreads as much as it seems likely to do. I read this on a msgs board with hundreds of other readers, which was only one of the many destination recipients of the intermediate link in the chain who remailed this.

First of all, let's assume this is an honest, innocent post, not a hoax of some sort. Let's note to begin with that as indicated by the mail cc's and headers, those "2 letters" which were sent out have already been multiplied a hundredfold across the internet by people who thought it was a cute idea. Let's note further, to our horror, that there is no date on the note indicating even when the "two weeks" is up. I'm very much afraid that this may go on for decades (if it hasn't already :-O).

In fact, by asking around, I've found that at least one posting of this note was sent out more than two weeks before the one I saw and copied here.

The general risks of the deliberate exploitation of wide e-mail distribution are obvious and have been discussed many times, but more specifically we can see a problem with an intended timed mailing for which the expiration date was either lost, modified, or never provided in the first place (as in this case).

Laurence R. Brothers ~ quasar@bellcore.com

↗ Access to psychiatric records

<Bob_Frankston@frankston.com>
Sat, 18 May 1996 14:11 -0400

There is an article in *The Boston Globe* 18 May 1996 entitled "AG to probe access to psychiatric records". As usual, one has to guess what is really going on and who is confused about what.

Apparently a local HMO has been including psychiatric records in its medical

history database. The first problem cited was the lack of effective access control on that portion of the records. The HMO claims to have "..installed software that limits access to the detailed notes ...".

The other problem is that, apparently, by placing the psychiatric history in the medical record it becomes available to insurance agencies once the patient has signed a release.

This seems to be a typical case of the computer forcing an issue that was already lurking. Medical records are medical records. It seems that it was an implicit (or even explicit) artifact of the paper system that the access was controlled and, perhaps, the insurance companies did not get access. And this was probably a good policy. But it might not have been legal if the insurance companies have access to all records.

As an aside, I think that under Massachusetts law that patient has access to all records which would presumably including the psychiatric transcripts. And records mean any scribbles. Am I wrong on this?

Is this a matter of an issue being forced by the computerization? Does that mean we must go back to shoeboxes so that records can be "lost" in order protect privacy?

↗ Smartcards and medical data standards

Peter Bray <"pabcse@airmail.net"@server.airmail.net>
Sun, 19 May 1996 10:21:42 -0700

There is a risk that the rapid and competitive evolution of Smart Card technology will result in a proliferation of data format standards that are proprietary or national in nature. In particular, information categories peripheral to financial transactions could suffer and the potential benefits go unrealized in the immediate term. Medical data, particularly physician to physician alerts and prescription medications and administration regimes are an example. What principles should govern the programme to develop such standards?: Keep it simple and extensible and end-use focused. Aim to keep it international and spoken language independent. Build in configuration management and downward compatibility as medicine and the delivery technology evolve. Include communication protocols for further information. Do not neglect promotion and training plans for practitioner's.

Peter Bray pabcse@airmail.net

↗ Re: Largest Computer Error in US Banking History? (RISKS-18.14)

"Louis Koziarz" <koziarz@mcs.com>
Wed, 22 May 1996 22:12:31 -0500 (CDT)

(From talking with a knowledgeable friend in the banking/ATM business:) The First National Bank of Chicago/Cash Station 'glitch' was apparently the result of a programming change intended to support the new out-of-area ATM fees being proposed by various banking groups. When the new transaction messages were introduced to the network, some systems took the strange new codes and transformed them into something they could understand: a posting of a huge credit to one's account.

The RISKs here may be more serious than the traditional glitches in electronic financial transactions. What should transaction-based systems do with unrecognizable or foreign input?

Risks of Statistics in RISKS-18.13

Frank Fay <f.fay@ieee.org>
Thu, 23 May 1996 12:06:01 -0700

Part 1 (Computer as Goat): Post-divorce wage gap statistic turns out to be computer error

This is a rather old story and computer errors are the least of the problems here. Readers wishing a fuller well-documented account should see Susan Faludi's book "Backlash" (1991), 1st edition, pages 19-25.

According to this account, Weitzman's book "The Divorce Revolution" was published in 1985, contains the -73%:42% figures (for reduction and increase in income after the 1st year of divorce), which are from a small sample size (114 men; 114 women) of interviews from a low response rate of the divorcing population in Los Angeles County. The financial information is based on the memory of those interviewed! As early as 1986 the findings were questioned by other divorce researchers whose own data indicated figures of -30%:10%-15% (close to the recent -27%:10% figures for re-analysis of Weitzman's data). Requests for Weitzman's data, for re-analysis, remained unfulfilled until late 1990 after appeals to the National Science Foundation.

According to the 1996 AP article Weitzman still cannot identify the source of the error ("She blames the loss of her original computer data file, a weighting error or a mistake in the computer calculations performed by a Stanford University research assistant."), and has left the re-analysis of her data to other researchers (Richard Peterson in this case).

As Faludi's extensively-documented book points out the conclusions of poorly conducted studies have real political and legal consequences. In addition they make "social science" more of an oxymoron, and hinder the efforts of those researchers who do good, repeatable work in these fields.

Part 2: Internet in danger (Nazi hate literature)

Jim Carroll seems to be misinterpreting the 80% statistic in several ways:

First, hate literature is likely a small fraction of all literature. Therefore 80% of a small number is an even smaller number.

Second, he should find out "what 80% means?". I have seen this figure in the past, and I believe the context is regarding published Nazi hate literature available by mail in Germany. I am not sure that the figure even includes e-mail or the Internet at all.

Third, the 80% of hate literature originating from Canada statistic does not imply "80% of Canadians" at all. Canada as a free-speech nation happens to be a convenient safe point from which to send this stuff. Furthermore this probably does not imply that the literature was written or published in Canada. I would suspect that a good deal of it comes from my country, the United States.

[See a recent Sunday New York Times Magazine cover article for more background.]

Frank Fay f.fay@ieee.org